IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Thomas J. Gilg	Group Art Unit:	2136
Serial No.:	10/719,724	Examiner:	Shanto Abedin
Filed:	11/21/2003		
For:	MICRO ELECTRONIC DEVICE WITH PLURALITY OF ENCRYPTION/DECRYPTION LOGIC		

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION UNDER 37 C.F.R. §1.131

We, Thomas J. Gilg and Ravi Prasad, being sworn do hereby state that:

1. We are joint inventors of claims 9-16 and 20-25 of the patent application identified above and the inventors of the subject matter described and claimed therein.

2. Prior to October 17, 2003, we conceived of and reduced to practice the invention as described and claimed in the subject patent application in this country. ***Exhibit A***, attached hereto, evidences our completion of the claimed invention prior to October 17, 2003.

3. The attached ***Exhibit A*** is invention disclosure information that we generated to document our invention prior to October 17, 2003.

By signing below, we declare that all statements made herein are of our own knowledge are true and that all statements made on information are believed to be true; and further that the statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application and or patents issued thereon.

January 7, 2008

Thomas J. Gilg
Thomas J. Gilg

January 2, 2008

Ravi Prasad

EXHIBIT A

Disclosure No. 200308974

Invention Disclosure - DBI Document No. 6BHD

invent

PD No.	Date Received	Collection
200308974		IPG

The information contained in this document is HP CONFIDENTIAL and may not be disclosed to others without prior authorization. Submit this disclosure to the HP Legal Department as soon as possible. No patent protection is possible until a patent application is authorized, prepared, and submitted to the Government.

General Information

Title Pixel-level security

Abstract We propose a display where security is implemented at the pixel (or pixel group) level rather than the whole-display level.

Security includes discovery of pixels, access rights to and from pixels, secure communication to and from pixels, and encrypted content flow to and from pixels.

Implementation includes pixel addressing schemes (programmatic and video file formats), and the physical implementation of security logic/circuitry next to the pixel logic/circuitry.

Projects Digital Projectors and New Business Creation

Description of Invention

Problems Solved Physical pixel-level (or pixel group) security solutions

Display security is typically implemented at the whole-display level of abstraction in a physically distinct subsystem (e.g. video driver chipset) from the light modulation subsystem (e.g. LCD or DLP panels). Between these subsystems is typically a single electrical interface, often sufficiently physically accessible to permit someone to "sniff the bits" flowing over the interface.

By moving the level of abstraction to the pixel level, and relocating and duplicating security circuitry to each pixel, there is no longer a single electrical sniff point.

Programmatic pixel-level (or pixel group) security solutions

No matter the physical implementation, moving the whole-display level of abstraction to the pixel level opens up several novel solutions.

1) Regions (to pixel or pixel group resolution) of a single physical display can be selectively advertised or seen.

Exampe - A teacher's presentation PC in a lecture hall can discover the entire display surface in the front of the lecture hall for subsequent use. Student presentation PCs in the same lecture hall can only discover a portion of the entire screen (the left hand side), to which they might post questions.

2) Regions (to pixel or pixel group resolution) of a single physical display can have varied read and write permissions.

Example - A bill board display in a public campground can have select regions that can only be written to by the campground maintainers. Other regions would be writable by all.

3) Regions (to pixel or pixel group resolution) of a single physical display can communicate securely.

Example - In a narrow casting application, both a region of the screen and the sending application can negotiate a secure communication channel so that instructions and content sent to the display cannot be sniffed in transit.

4) Regions (to pixel or pixel group resolution) of a single physical display can engage in differing encryption/decryption strategies and keys.

Example - You wish to download a Hollywood movie in digital form, but Hollywood does not want your copy to work on anyone else's display. Therefore, each pixel (or pixel group) in your display can generate a unique public encryption key which gets communicated to Hollywood, and Hollywood encodes digital video that can only be decrypted by the pixels of your display.

Example 2 - A military application of the above.

Example 3 - Combine this with physical pixel-level security.

Description For physical, additional circuitry is located next to each pixel (or pixel group), and this circuitry can be uniquely addressed.

For programmatic, its a matter of software programming.

Advantages Pixel level security is harder to sniff, and opens up new display-interaction paradigms.

Inventor Information

Inventors [redacted]

Thomas J Gilg | **Hewlett-Packard Company** | **Corvallis**

00308790 Americas (6480-5000)

4861 SW Roseberry Street
Corvallis, OR 97333
United States [US]

+1 (541) 715-2756
thomas_gilg@hp.com
United States [US]

Ravi Prasad | **Hewlett-Packard Company** | **Corvallis**

00502308 Americas (6410-5393)

2870 NW Satinwood Street
Corvallis, OR 97330
United States [US]

+1 (541) 715-8898
ravi_prasad@hp.com
United States [US]

Witnesses

Witnesses

Jon A Brewster | **Hewlett-Packard Company** | **Corvallis**

Americas (6480-5000)

jon.brewster@hp.com +1 (541) 715-4483

Steve Froelich | **Hewlett-Packard Company** | **Corvallis**

Worldwide (0000-7709)

steve_froelich@hp.com +1 (541) 715-2710

Classification

Recommended Classification IPG: Emerging Technologies: Display Technology

Administrative Record

Date Submitted

Legal Clerk **Jessica Jessica Fusek** | **Hewlett-Packard Company** | **San Diego**

_______________, __________, ________, ________
(0000–103)
jessica_fusek@non.hp.com +1 (208) 396-3575

PD Number 200308974

Date Received by Legal

Wendy A. Balabon

From: GILG,THOMAS J (HP-Corvallis,ex1) [thomas_gilg@hp.com]
Sent:
To: Wendy A. Balabon
Cc: Michael R. Bascobert; Glenn E. Forbis
Subject: RE: U.S. Patent Application " Pixel-Level Security"; HP No. 200308974; Our Ref. No.; 65079-0076

Michael,

As expected, your write-up is causing me to better articulate all the major elements of my disclosure.

Let me start by saying that I will use the word "picture" to include A) digital still images (e.g. TIF, JPEG) and B) digital video images (e.g. MPEG2, h.261). This disclosure applies equally well to both classes of pictures.

There are really two distinct concepts I need to call out:

1) Current picture encryption/decryption techniques are applied at the whole picture level. If you have a 5x4 picture, a single encryption step will consume all 20 pixels at once, without significant regard to their spatial placement, and encrypt them into a blob. Once transmitted to the display side, a single ~~decryption~~ step will consume the blob at once, and will regenerate the 20 pixels.

My disclosure is that encryption and decryption activity can occur at the pixel level or pixel-region (sub-display) level, in addition to the "whole display" level.

See the attached slide deck and the slide titled "Multi-Key Concept".

Some relevant notes on this concept.

- There are a number of well-known encryption/decryption techniques involving one key or matched public-private keys. This disclosure works with all of these encryption/decryption techniques.

- The source and destination devices can either have a fixed notion of the encryption/decryption regions, or can exchange a trivial descriptor of the encryption/decryption regions.

In the example with 10 key regions, the descriptor could be:

1,1 / 1,2 / 1,3 / 1,4 / 1,5 / 2,1 / 2,2-5 ; 3,2-5 /
2-3,5 ; 4,2-5 / 3,1 / 4,1

Coordinates are expressed using "x,y", ranges of contiguous values can be expressed using "-", a "/" delineates the coordinates contained in a key region, and a ";" delineates the portions of a key region.

- The slide "Multi-Key Concept 2" shows that not all displays might have access to all the region keys, therefore is unable to decrypt some regions.

- While my emphasis has been on the display side, there is a corresponding element on the source side. Pixel level or pixel-region level security for display and capture devices.

2) Current picture encryption/decryption techniques are implemented in circuits that are not close-to or integral-to a pixel's immediate circuitry (e.g. LCD, Plasma, not CRT). For example, a digital video projector typically has a printed circuit card that contains all image processing and decryption circuits, and the output (unencrypted pictures!) of such a card is typically conveyed to the display circuit via a ribbon cable or physical connector, and is easily tapped into by hackers.

My disclosure is that a much more robust and secure system is made when the act of decryption is implemented by circuits associated with each pixel, or in circuits that drive a small region of pixels. For example, each pixel in an LCD display has one or more transistors physically associated with it (less that 1mm away) for the sake of sensing the addressing matrix and then driving the pixels light state. Emerging manufacturing techniques now make it possible to associate more complex circuitry with each pixel, such as decryption circuitry.

Some relevant notes:

- An extremely secure display could be built by implementing a public/private key generator circuit at the pixel or pixel-region level. The display would release all the public keys so that content authors could properly encrypt picture content for the display (using the various public keys), but the private keys would never be released by the pixel or pixel-region circuits. Literally no one outside of the pixel or pixel-region would know how to decrypt incoming pictures. Hacking would require complex probing into each pixel or pixel-region curcuit.

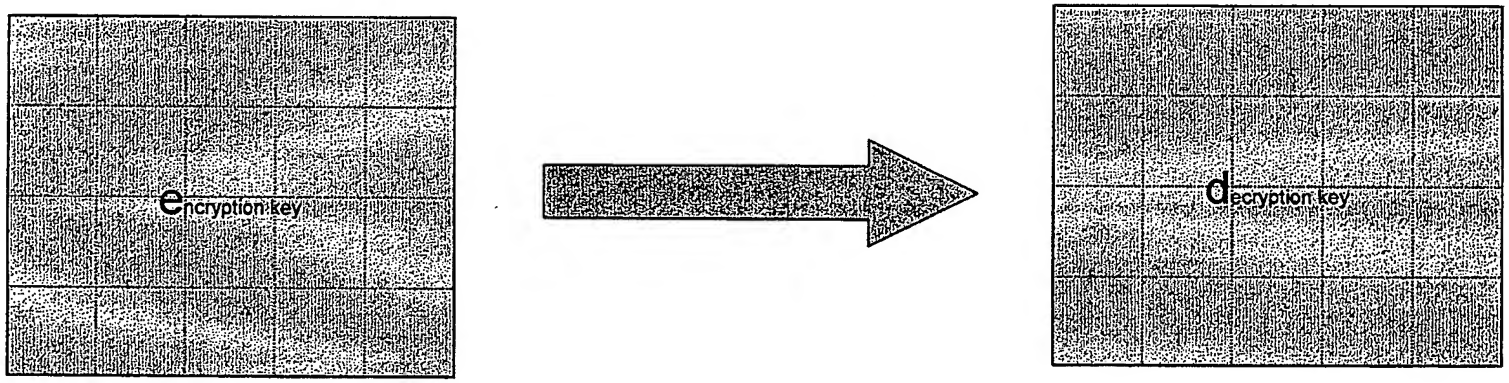
I will resume my review and commentary on Tuesday morning.

Thomas Gilg

5x4 Display Example – Multi-key Concept

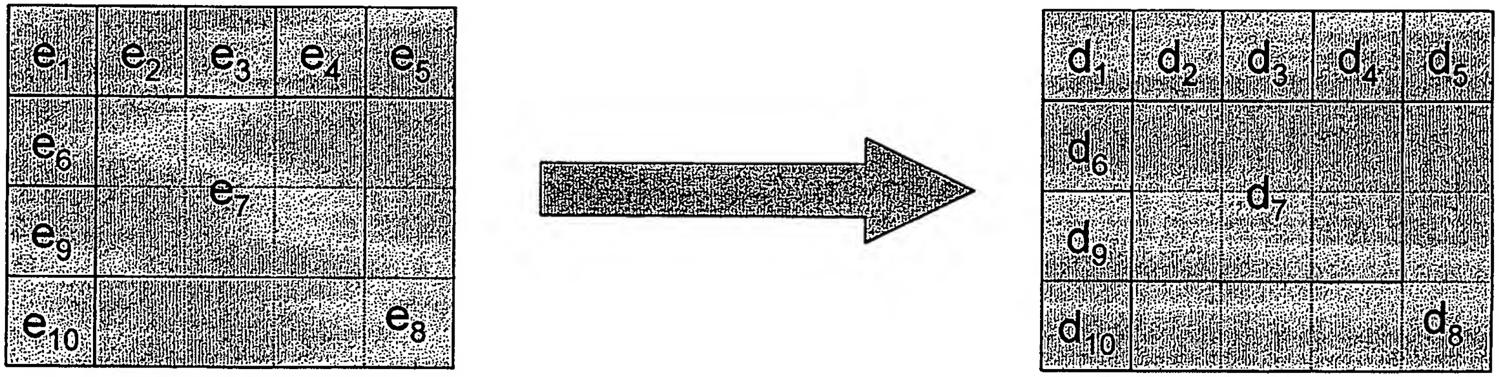
today's "whole display" encryption/decryption example

(one single-key or one public/private-keys)



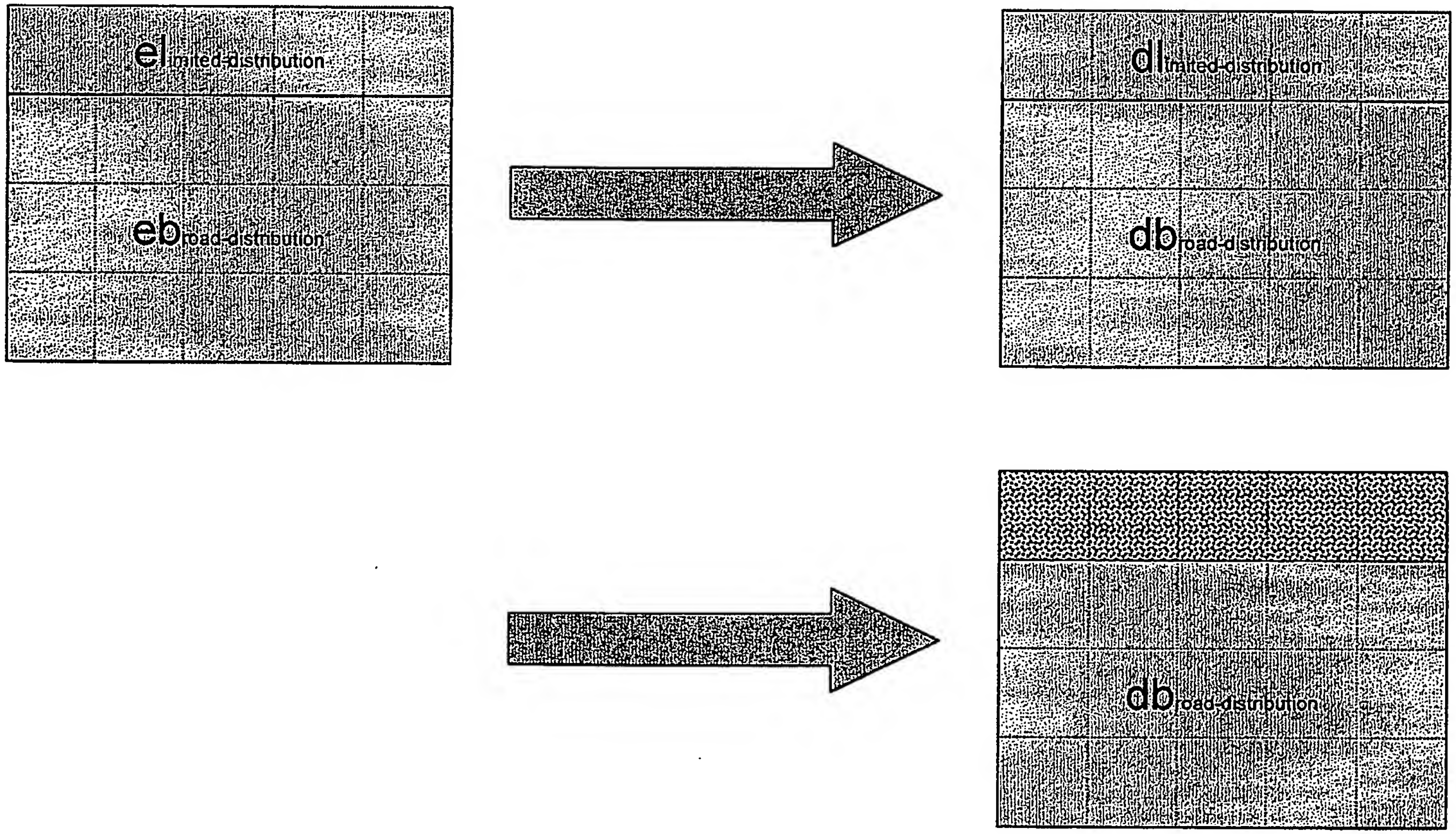
mixed "pixel and pixel-region" encryption/decryption example

(multiple and unique single-key or multiple and unique public/private-keys)



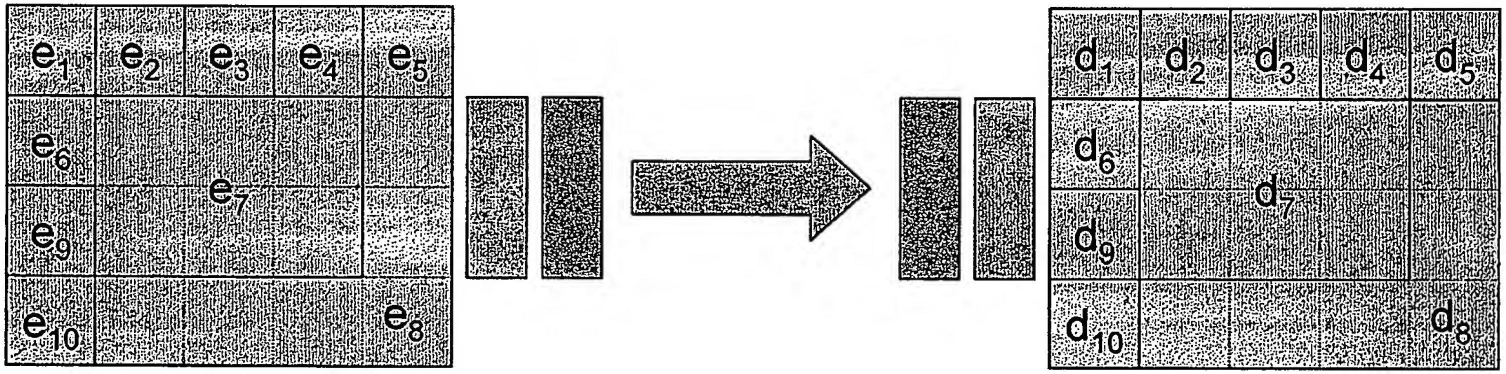
5x4 Display Example – Multi-key Concept 2

one display has access to both regions, while another display only has access (privilege) to the lower region for lack of knowing the upper regions decryption key

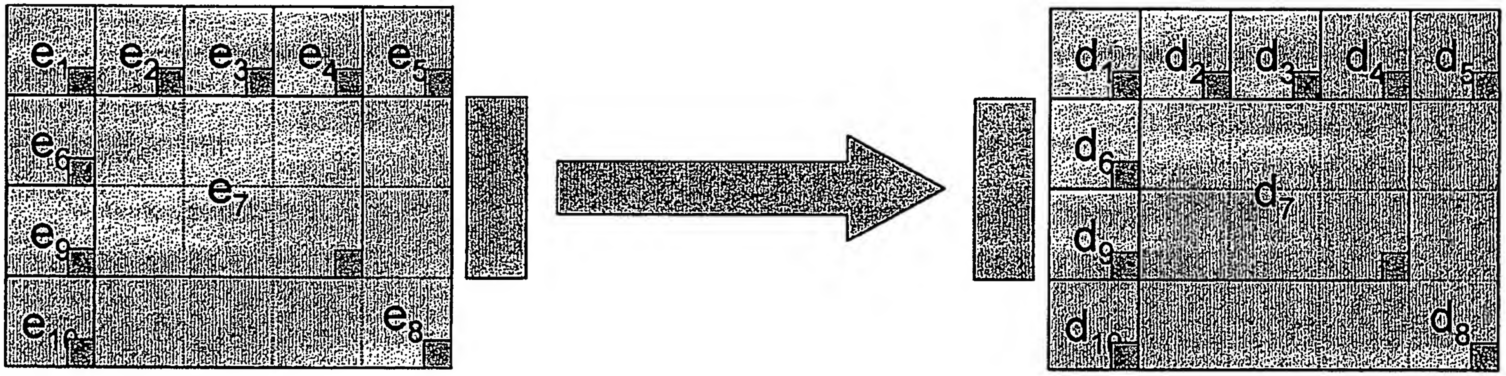


5x4 Display Example – Robust Implementation Concept

today's "not integral" encryption/decryption example



"integral" encryption/decryption example



Orange – encoder/decoder circuit
Purple – pixel signal distribution wires and circuits